УДК 004.056

Ю.І. Петришин
Тернопільський національний університет імені Івана Пулюя, Україна

КЛАСИФІКАЦІЙНІ ОЗНАКИ СТЕГАНОГРАФІЧНИХ МЕТОДІВ

Y.I. Petryshyn

CLASSIFICATIONS STEGANOGRAPHY TECHNIQUES

Сучасний інтерес до стеганографії, як сукупності методів приховування інформації, виник у значній мірі завдяки інтенсивному впровадженню і широкому розповсюдженню засобів обчислювальної техніки в усі сфери діяльності людини. Це дозволяє активно застосовувати всі переваги, які дають стеганографічні методи захисту.

Проаналізувавши існуючі на даному етапі методи прихованої передачі інформації можна запропонувати підхід для класифікації методів комп'ютерної стеганографії. Всі існуючі методи розділимо на такі групи: вибір контейнера, наявність ключа, призначення, принцип приховування, стійкість. За вибором контейнера.

Вибір контейнера можна розділила за п'ятьма напрямами:

1.По формату:

а) спеціальне форматування текстових файлів;

б) використання зарезервованих для розширення полів комп'ютерних форматів даних;

в) використання надлишковості аудіо та візуальної інформації.

2. За способом вилучення інформації:

а) з оригіналом;

б)без оригіналу;

в) по фрагменту оригіналу.

3. За розміром контейнери бувають:

а) потоковими – до них відносяться контейнери, розмір який наперед невідомий і може змінюватись під час приховування інформації.

б) фіксованими – до них належать контейнери розмір яких наперед відомий і незмінний.

На практиці частіше за все використовуються саме контейнери фіксованої довжини, як найбільш поширені і доступні.

3.По способу вибору контейнера:

а) в сурогатних методах стеганографії повністю відсутня можливість вибору контейнера і для приховування повідомлення вибирається перший ліпший контейнер;

б) в селективних методах КС передбачується, що приховане повідомлення повинне відображати спеціальні статистичні характеристики шуму контейнера;

в) в конструюючи методах стеганографії контейнер генерується самою стеганосистемою;

4. По способу організації контейнери, подібно завадостійким кодам, можуть бути

а) систематичними, в яких можна вказати конкретні місця стеганограми, де знаходяться інформаційні біти контейнера, а де шумові біти, призначені для приховування інформації.

б) несистематичні, в яких все навпаки.

5. За наявністю ключа стеганосистеми поділяються на: ключові, без ключові, змішані.

Для функціонування безключових стеганосистем, крім алгоритму стеганографічного перетворення, немає необхідності в додаткових даних, на подобі стеганоключа. Ключові стеганосистеми поділяються на системи з секретним та відкритим ключами. Для систем з наявністю секретного ключа необхідна наявність безпечного (захищеного) каналу обміну стеганоключами. Стеганографічні системи з відкритим ключем не мають необхідності в додатковому каналі ключового обміну. Для їх функціонування необхідно мати два стеганоключа: один секретний, який необхідно тримати в таємниці, а інший – відкритий, який може зберігатися в доступному для всіх місці. За призначенням стеганографічні методи можна розділити на такі області використаня: захист від копіювання (електронна комерція, контроль за тиражуванням (DVD), розповсюдження мультимедійної інформації); прихована анотація документів (медичні знімки, картографія, мультимедійні бази даних); аутентифікація (системи відео спостереження, електронної комерції, голосової пошти, електронне конфіденційне діловиробництво); прихований зв'язок (використання в воєнних розвідувальних цілях, а також у тих випадках, коли використовувати криптографію заборонено).

Використання стеганографічних систем є найбільш ефективною при вирішенні проблеми захисту інформації з обмеженим доступом. Крім прихованої передачі повідомлень, стеганографія є одним з найбільш перспективних напрямів для аутентифікації і маркування авторської продукції з метою захисту авторських прав на цифрові об'єкти від піратського копіювання.

Нерідко методи стеганографії використовують для камуфляжу програмного забезпечення. У тих випадках, коли використання програм незареєстрованими користувачами є небажаним, воно може бути закамуфльоване під стантартні універсальні програмні продукти (наприклад, текстові редактори) або приховане у файлах мультимедіа (наприклад, у звуковому супроводі комп'ютерних ігор).

Також стеганографічний підхід використовується при створенні прихованого каналу витоку чутливої інформації від санкціонованих користувачів.

По принципу приховування методи комп’ютерної стеганографії діляться на два основні класи: безпосередньої заміни і спектральні методи. Якщо перша, використовуючи надлишок інформаційного середовища в просторовій або часовій області, заключається в заміні малозначущої частини контейнера бітами секретного повідомлення, то інші для приховування даних використовують спектральне представлення елементів середовища, в яке вбудовують приховувані дані.

За стійкістю можна виділити робастні, вразливі та напіввразливі стегосистеми. Пояснити таку класифікацію можна за допомогою цифрових водяних знаків (ЦВЗ).

Під робастністю розуміється стійкість ЦВЗ до різного роду впливів на стего. Робастності ЦВЗ присвячено більшість досліджень. Вразливі ЦВЗ руйнуються при незначній модифікації заповненого контейнера. Вони використовуються для підтвердження сигналів. Напіввразливі ЦВЗ стійкі по відношенню до одних дій і нестійкі по відношенню до інших. Напіввразливі ЦВЗ спеціально проектуються так, щоб бути нестійкими по відношенню до певного роду операцій.

На нашу думку такі класифікаційні ознаки найбільш широко відображають систему методів прихованої передачі інформації. Цей спосіб не вказує на самі методи, тут немає жодної конкретної назви того чи іншого методу, проте тут відображені всі основні властивості, які необхідно враховувати при вирішенні тієї чи іншої задачі.